Monthly Security Tips Newsletter
February 2008

CISO Tips

*ALERT: Several new/updated policies/standards/guidelines are pending. Please watch for the updates and thoroughly review for impact.

Trojan malware installed on customer PCs, in the form of key-loggers, are very common. Where applicable on your Web sites, please make your customers aware of the possibility in order to combat loss of sensitive data.

Remember to protect your home computer from access to unsafe and undesirable sites. If you have children (or not), try Blue Coat's™ free home offering at http://www1.k9webprotection.com/;

To view State security policies, please visit: http://isd.alabama.gov/policies/policies.aspx?sm=c_a;

Securing a Wireless Network

Is a Wireless Network Secure?
Wireless networks are not as secure as the traditional "wired" networks, but you can minimize the risk on your wireless network (at home or at work) by following the tips below.

How Does it Work?
The standard set up for a wireless network requires two components: a Wireless Access Point (WAP) and a computer with a wireless network adaptor. Properly configuring a wireless device can be challenging and the steps will vary depending on the manufacturer. If you do not feel comfortable doing it yourself, be sure that whomever is configuring the wireless network follows these best practices.

Wireless Access Point (WAP)
The WAP connects to your high speed Internet connection or your internal network. This is the foundation for building a wireless network. It provides the ability to use a computer without being constrained by the distance of a wire. Keep in mind that metal filing cabinets as well as certain building materials, such as bricks and blocks, can interfere or limit the range. The distance between your wireless computer and the wireless access point [can affect signal strength]. Generally, the indoor range for a WAP is approximately 125 feet.

Wireless Network Adaptor
A wireless network adaptor, used for transmitting and receiving information, is required for each computer you intend to connect to a WAP. When purchasing wireless networking hardware from separate vendors, be sure to obtain guarantees that the hardware will conform to defined standards and interoperate properly. The wireless network adaptor is usually built into laptop computers while it is an add-on component inserted into a USB port on desktop computers.

Enable Encryption
Every wireless network should enable encryption. Encryption scrambles the data in a way that if your signal is intercepted there is reduced risk of someone being able to eavesdrop or monitor your communications. There are several standards of encryption common to most WAPs. Wired Equivalency

Privacy (WEP) is the older standard. WEP has a number of known security flaws and should only be used if no other method of encryption is available. Be sure to set the WEP authentication method to "shared key" instead of "open system." Under "open system" the initial sign-on is encrypted but the data is not. Newer wireless access points include Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access 2 (WPA2). WPA2 is stronger and the preferred method of encryption.

Change the Default Password

Change the default password that comes with your WAP. The default passwords used by manufacturers are well known to the hacking community. Be sure to use a strong password, at least eight characters including numbers and special characters.

Change SSID Name

The Service Set Identifier (SSID) is the name of your wireless network. Default SSIDs are well known, often the name of the manufacturer and easy to guess. Change the SSID name to something unique and be careful not to use a name that freely discloses information. For example, avoid using your family name. Avoid descriptive or functional names as well, such as "Payroll" or "Accounting" since this would advertise an attractive target for an attacker.

Turn Off SSID Broadcasting

By turning off SSID Broadcasting, your wireless access point does not advertise its presence. It is similar to having an unlisted telephone number. This is a way to reduce the visibility of your network to others in your neighborhood. The only way to connect to a WAP with SSID Broadcasting turned off is to know the SSID name and password.

Use MAC Filtering on Your WAP

The MAC (Media Access Control) address is the unique ID assigned to your computer's network interface card. It is referred to as the computer's "physical address." Enabling MAC filtering on your WAP allows you to designate and restrict which computers can connect to your WAP. If the computer's address is not listed, a wireless connection cannot be made to the WAP. To look up a MAC address on a Windows computer, go to "Start" then "Run" and type "cmd". A new window will open and you will need to type ipconfig /all and press the enter key. A number of attributes will be displayed. The MAC address is identified as the "Physical Address."

RF Interference

Assuming your WAP point functions in the 2.4 GHz range, you may experience Radio Frequency (RF) interference from other 2.4 GHz devices, such as cordless phones, microwaves and baby monitoring devices. These devices can limit wireless performance. To manage the problem, limit sources of RF interference in proximity to the WAP.

Additional resources for Wireless Networks can be found at:

- Wireless Network Tutorial including manufacturer step by step procedures: http://spotlight.getnetwise.org/wireless/wifitips/
- Microsoft**:** www.microsoft.com/technet/network/wifi/wifisoho.mspx
- US CERT: www.us-cert.gov/cas/tips/ST04-014.html

For more monthly tips visit: www.msisac.org/awareness/news/

MS-ISAC

http://www.msisac.org